Anomali Malware Intelligence

Out of The Box Fresh Malware Intelligence

Security teams are under increasing pressure to do more with less. Unfortunately, most organizations struggle with effectively implementing threat intelligence, not benefiting from the value their threat intelligence team, processes, and tools provide.

Anomali's Malware Intelligence Feed is here to help.

A real-time, global, curated feed of approximately 50,000 daily malware samples from over 300+ prominent malware and ransomware families. All of the contents are sandboxed in order to provide greater accuracy and context to support effective automation and greater efficiency of analyst resources.

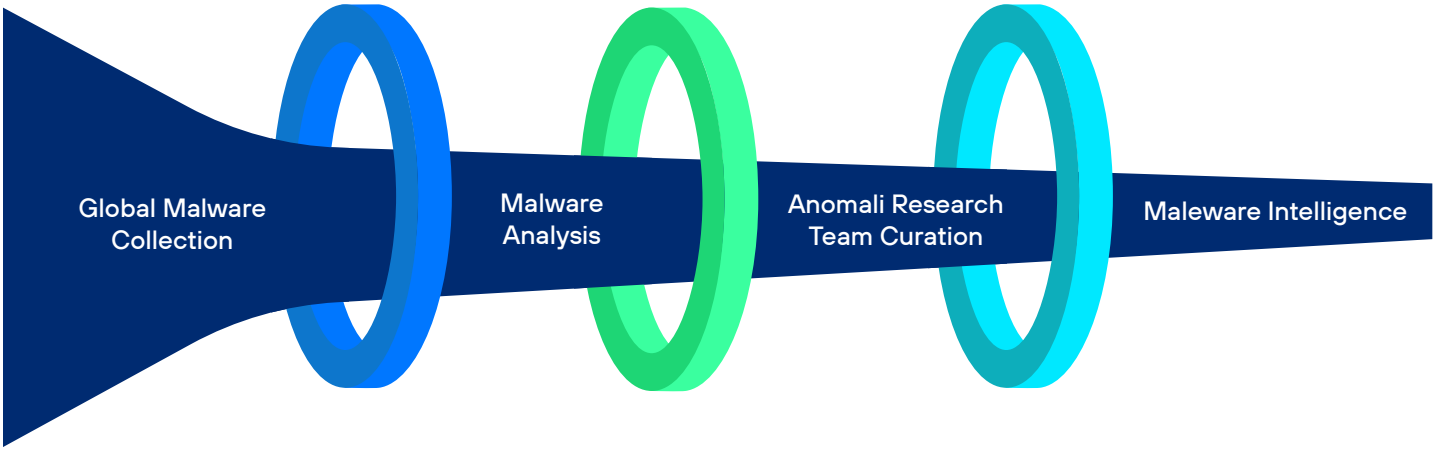
This global malware feed is a must-have for threat intelligence teams with limited resources who want to proactively protect their infrastructure, supply chain, and customers.

Powered by PolySwarm's incentive-based marketplace, the feed enlists an extensive global network of technologies from expert malware researchers with additional cu ration by the Anomali Threat Research team.

Continuous, fresh intelligence enables security teams to aggregate, manage, and operationalize responses to malware threats in their environment at a fraction of the cost of other malware feeds.

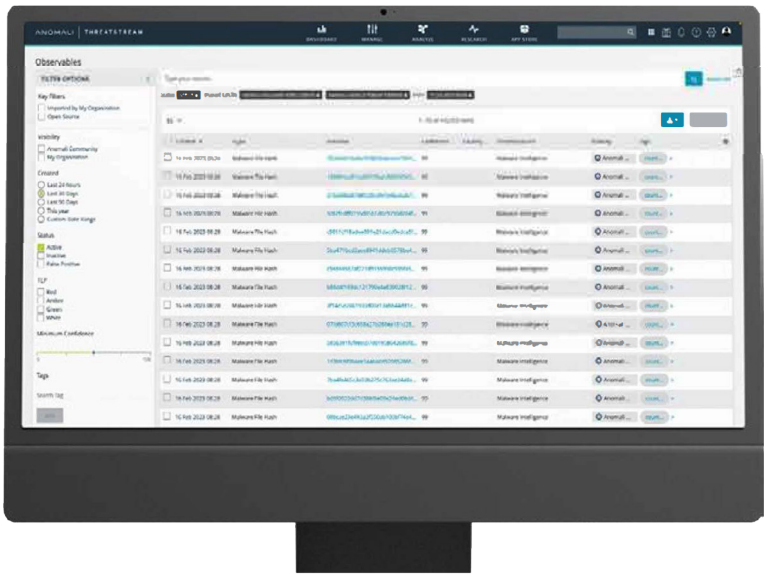
DRIVING BUSINESS VALUE

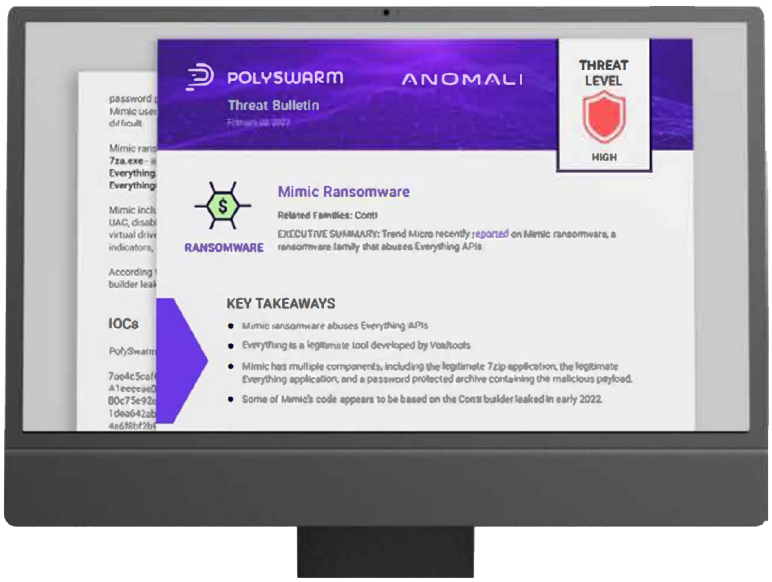
- Increased visibility and early warning of targeted threats
- Reduced exposure to potential breaches
- Increased productivity and reduced burnout of Threat Intelligence and SOC Teams
- Increased SIEM/SOAR R.O.I.
- Streamline CTI team workflows
- Value pricing extends the capabilities of CTI and SOC Teams



KEY PRODUCT BENEFITS

- Global malware coverage
- Ready to go malware intelligence for Security Teams
- Global malware coverage 100% sandboxed
- Detailed C2 information
- Extensive tagging for effective automation and team analysis
- Unified Malware naming
- Integrated Risk Scoring directly in Threatstream
- Mitre TTP support
- Premium Malware Threat reports





PREMIUM MALWARE THREAT REPORTS

- Use in conjunction with Anomali + Polyswarm DashBoard Feed
- Gain Valuable Insights and Context that are actionable
- Uncover specifc industry and geography related issues published 2-3x per week

Key Use Cases

SOC Automation

Detailed threat scoring and tagging drive actionable automation

Threat Hunting

Fresh malware from over 300+ malware/ ransomware families

Telemetry enrichment

Comprehensive tagging and C2 information

Incident Response

Mitre TTP details and extensive tagging

Vulnerability management prioritization

CVE information along with numeric threat scoring

ANOMALI